20 February 1997

Version Description Document

Defense Information Infrastructure (DII)

Common Operating Environment (COE)

Tivoli Management Environment Segments

TIVSRV V3.0.0.5 (Parent Segment) with
TMPSRV, ADMSRV, SENSRV & COUSRV V3.0.0.5 (Child Segments)

TIVCLT V3.0.0.5 (Parent Segment) with
TMPCLT, ADMCLT, SENCLT & COUCLT V3.0.0.5 (Child Segments)

Prepared by:

The MITRE Corporation
202 Burlington Road
Bedford, Massachusetts 01730

SECTION 1

SYSTEM OVERVIEW

The Tivoli Management Environment provides client-server services for managing heterogeneous workstations and other desktop systems. The Tivoli Management Environment is compliant with the Object Management Group's Common Object Request Broker Architecture (CORBA). The Tivoli Management Environment (TME) consist of the following:

- Tivoli Management Platform V3.0.1
- Tivoli/Admin V3.0
- Tivoli/Courier V3.0
- Tivoli/Sentry V3.0

The TME segments consists of the following:

- TIVSRV V3.0.0.5 (Parent Segment)
  - TMPSRV V3.0.0.5 which consists of the server portion of the Tivoli Management Platform (Child Segment)
  - ADMSRV V3.0.0.5 which consists of the server portion of Tivoli/Admin, (Child Segment)
  - SENSRV V3.0.0.5 which consists of the server portion of Tivoli/Sentry, (Child Segment)
  - COUSRV V3.0.0.5 which consists of the server portion of Tivoli/Courier, (Child Segment)
- TIVCLT V3.0.0.5 (Parent Segment)
  - TMPCLT V3.0.0.5 which consists of the client portion of the Tivoli Management Platform (Child Segment)
  - ADMCLT V3.0.0.5 which consists of the client portion of Tivoli/Admin, (Child Segment)

- SENCLT V3.0.0.5 which consists of the client portion of Tivoli/Sentry, (Child Segment)

- COUCLT V3.0.0.5 which consists of the client portion of Tivoli/Courier, (Child Segment)

The Tivoli Management Environment is a commercial product that provides a comprehensive set of services for administering systems. Tivoli expands system administrators' effectiveness by permitting common system administration functions to be performed remotely. Tivoli supports all current major vendor platforms and provides the same user interface across platforms, thus, reducing the need for system administrators to be trained in individual platform administration.

The Tivoli Management Platform (TMP) encompasses the fundamental set of CORBA capabilities that all Tivoli functions use, as well as a set of basic system administration tools. The CORBA capabilities will be transparent to most Tivoli users. The basic system administration tools are accessible via a graphical user interface or via the command line. These system administration tools include the following:

- Administrator management. Tivoli administrators are explicitly defined using Tivoli's administrator management functions. An administrator's definition includes the system administration resources the administrator is allowed to access, as well as the privileges allowed when accessing those resources. Privilege enforcement is done via roles, where each Tivoli role has a predefined set of privileges associated with it, using a Kerberos model. This means of role-based access control enables system administrators to perform administration functions without requiring the root password.

- Notification groups. Tivoli's notification groups provide a log of administrator activity. Tivoli applications record administrator actions into application-specific notification groups. These notices provide an administration-specific audit trail.

- Profiles and profile managers. Tivoli manages common system resources according to a resource template, called a profile. A profile captures the attributes of a specific resource that Tivoli will manage. User accounts, host namespace (IP address assignment) are examples of resources managed via profiles (as part of the Admin product). The profile includes the definition of rules (see policy regions) that will be enforced for the profile attributes, such as the user password criteria. A collection of one or more profiles are contained within a profile manager. Profile managers can be used to group profiles of a similar type, or to group profiles that only apply to specific subscribers.

- Basic managed node. Installing a Tivoli client on a system makes that system a Tivoli managed node. This permits Tivoli to perform remote management actions

on that node, including querying its physical and logical configuration without having to log into that node.

- Policy regions. Policies are rules that will be enforces for system administration. Tivoli provides two types of policies: default policy, invoked when a new instance of the resource is created (e.g., user); and validation policy, used to check that existing resources still comply with the rules. Resources that have a common set of policies reside in a policy region, a group of resources that share common rules. Tivoli permits nested policy regions so that policy regions can reflect a model of the organization.

- Inter-TMR connection. TMRs can be interconnected to provide scalable system administration and to reduce the effects of individual management server failure.

- Tasks and jobs. A Tivoli task is an administrative procedure that has defined for one or more platforms and placed in a task library. The task definition includes the roles required to run the task. Thus, Tivoli tasks permit common system administration tasks, such as removing core files, pruning out unused user accounts, or checking for invalid user passwords, to be performed securely. A job is a Tivoli task that has been predefined to run on specific managed nodes.

- Scheduled actions. A common part of system administration is that certain actions have to be performed at regular intervals or at off-hours so that they do not interfere with mission-critical operations. Tivoli provides a scheduler to support this, with role and privilege enforcement associated with it.

Tivoli Admin uses Tivoli's profile capability to provide user, group and, host namespace management. Tivoli Admin also provides NIS and NIS+ domain management. Tivoli Admin's main functions are as follows:

- User account management. Tivoli supports adding, editing, and deleting user accounts, as well as distributing user account information to other profile managers, to managed nodes (updating the /etc/passwd file), and to NIS and NIS+ domains.

- Group management. Tivoli supports adding, editing, and deleting Unix groups, as well as distributing group information to other profile managers, to managed nodes (updating the /etc/group file), and to NIS and NIS+ domains.

- Host namespace. Tivoli supports adding, editing, and deleting host name-IP assignments, as well as distributing host namespace information to other profile managers, to managed nodes (updating the /etc/hosts file), and to NIS domains.

- NIS. Tivoli supports adding, editing and deleting NIS maps and map data, as well as making and pushing NIS maps.

- NIS+. Tivoli supports the distribution of user and group profiles in a NIS+ environment.

Tivoli Sentry provides a secure, distributed, general-purpose system monitoring capability. It does not require polling to detect changing conditions on clients, as Tivoli Sentry monitors run locally, that is, on the managed node being monitored. Sentry also implements role and privilege definitions to control which administrators are permitted to define or modify Sentry monitors.

When a Sentry condition is detected, Tivoli Sentry can be configured to take corrective action automatically, send e-mail, notify specific administrators, or run an executable. If needed, Sentry can work in concert with SNMP, and can receive SNMP traps via asynchronous Sentries.

Tivoli Courier provides software distribution (and removal) across heterogeneous platforms with a wide number of options, including repeater capability to reduce traffic over wide-area networks (local fan-out), single source to many destinations in a single action and pre or post processing.

SECTION 2

REFERENCED DOCUMENTS

The following documents are referenced in this VDD.

- Tivoli/Admin Release Notes V3.0, May 21, 1996
- Tivoli/Courier Release Notes (Rev B) V3.0 August 22, 1996
- Tivoli/Sentry Release Notes V 3.0 (Rev A), June 1, 1996
- Tivoli Management Platform Release Notes V3.0.1, June 28, 1996
- Tivoli Management Platform User's Guide
- Tivoli User and Group Management Guide
- DII COE Integration and Run Time Specification (I&RTS), Version 2.0, October 23, 1995.
- DII COE Security Software Requirements Specification (SRS), Version 2.0, July 8, 1996.
- DII COE Management Services SRS, Version 1.4, July 8, 1996.
- DII COE Security Manager Administrators Guide, Draft 1, 26 August, 1996.

SECTION 3

VERSION DESCRIPTION

3.1 Inventory of Materials Released

- Magnetic Media: 8mm tape consisting of TIVSRV V3.0.0.5 (Parent Segment) with TMPSRV V3.0.0.5, ADMSRV V3.0.0.5, SENSRV V3.0.0.5, and COUSRV V3.0.0.5 (Child Segments) and TIVCLT V3.0.0.5 (Parent Segment) with TMPCLT V3.0.0.5, ADMCLT V3.0.0.5, SENCLT V3.0.0.5, and COUCLT V3.0.0.5 (Child Segments) for DII COE V3.0 on Solaris 2.4.

- Magnetic Media: 8mm tape consisting of TIVSRV V3.0.0.5 (Parent Segment) with TMPSRV V3.0.0.5, ADMSRV V3.0.0.5, SENSRV V3.0.0.5, and COUSRV V3.0.0.5 (Child Segments) and TIVCLT V3.0.0.5 (Parent Segment) with TMPCLT V3.0.0.5, ADMCLT V3.0.0.5, SENCLT V3.0.0.5, and COUCLT V3.0.0.5 (Child Segments) for DII COE V3.0 on Solaris 2.4.

- Version Description Document for the Defense Information Infrastructure (DII) Common Operating Environment (COE) Tivoli Management Environment Segments, 7 October, 1996

- Software Test Plan for the Defense Information Infrastructure (DII) Common Operating Environment (COE) Tivoli Management Environment Segments, 7 October, 1996

- Software Test Description for the Defense Information Infrastructure (DII) Common Operating Environment (COE) Tivoli Management Environment Segments, 7 October, 1996

- Installation Procedures for the Defense Information Infrastructure (DII) Common Operating Environment (COE) Tivoli Management Environment Segments, 7 October, 1996

- Tivoli/Admin Release Notes V3.0, June 28, 1996

- Tivoli/Courier Release Notes (Rev B) V3.0, August 22, 1996

- Tivoli/Sentry Release Notes V 3.0, June 28, 1996

- Tivoli Management Platform Release Notes V3.0.1, June 28, 1996
- Tivoli Management Platform Documentation Package
- Tivoli/Admin Documentation Package
- Tivoli/Courier Documentation Package
- Tivoli/Sentry Documentation Package

3.2 Software Changes

Version 3.0.0.5 of the Tivoli Management Environment segments are an upgrade to the v3.0.0.4 of the segments. The new release incorporates the modifications which were addressed by the Errata for the Tivoli Managed Node (TMPCLT) v3.0.0.4. The errata discusses the failure of the Tivoli icon to appear on the desktop following the installation of the TMPCLT segment. Therefore, the Tivoli application could not be activated through the Common Desktop Environment (CDE) but instead would have to be activated through a UNIX command line. In addition, v3.0.0.5 includes an updated Installation Procedures document.

The following paragraphs discuss several important features in the Tivoli Management Environment segments v3.0.0.x (COTS version V3.x) which were specifically addressed due to concerns expressed by the DII COE Engineering Office.

3.2.1 Deployment and Tivoli Management Regions (TMRs)

Tivoli V3.0 will support ad-hoc assignments in new and existing Tivoli Management Regions (TMRs) with no risk of conflict. In past versions, when TMRs were re-deployed, there was a risk that the TMR ID could conflict since Tivoli assigned TMR IDs based on the license key. This is no longer the case; the algorithm now uses the hostname, IP address, time of installation and a random "seed" value to generate the TMR ID. This change eliminates the risk of conflict and makes redeployment of TMRs a simple task.

Before or after redeployment, systems can be added or removed from TMRs using existing, standard product capabilities. This provides flexibility during redeployment in cases where TMR's need to be combined or reduced/extended in size prior to being deployed to a new location.

3.2.2 User and Group Management in the NIS+ Environment

Tivoli supports both user and group management in a NIS+ environment out-of-the-box which allows Tivoli Admin to populate and distribute user and group profiles to NIS+ databases. Appendix F of the Tivoli User and Group Management Guide provides step-by-step instructions on how to configure NIS+ and NIS+ endpoints for TME.

3.2.3 Windows NT Support

The Tivoli Management Framework has been redesigned to run natively on Windows NT. Unique features in the Windows NT operating system have been exploited to enhance the performance and security of TME for Windows NT. The significance of porting the Tivoli framework to Windows NT is twofold. First and foremost, the port brings the full power of distributed object technology to Windows NT environments. Secondly, Windows NT can now be used as a management server. With TME for Windows NT, you can manage a homogeneous Windows NT environment as well a mixed environment of Windows NT, UNIX, NetWare and PC clients.

Tivoli Admin v3.0 introduces the first management application designed specifically to solve the problem of cross-platform and cross-resource account management. It provides the ability to manage Windows NT Registry, NetWare Directory Services and UNIX accounts from a single, integrated console. The user interface provides a consistent approach and look-and-feel and enables administrators to keep a single, consistent set of account information for users across the enterprise. This gives users a single sign-on to all of the resources they need to perform their jobs.

TME for Windows NT provides the ability to manage Windows NT and Windows 95 "profiles." A new concept in Windows user access management, profiles enable the definition and management of access to local and networked resources. Administrators use profiles to configure custom desktops for an individual user or a group of users, thus achieving fine-grained control over user access control privileges.

Tivoli Courier v3.0 adds a set of features that specifically target the Windows NT environment. The application has been "inventory-enabled" to facilitate this requirement. A query against the inventory database to check on the dependencies of application components creates a subscription list for the software package that makes distribution error-free. Tivoli/Courier includes a scriptless, automated installation procedure that uses technology licensed from Intel's LANDesk product. This technology eliminates written scripts, and the shrink-wrapped package can be automatically and remotely installed without user intervention. In addition, Tivoli/Courier provides an end-user pull interface that gives mobile users the ability to hook up to a server and pull down the latest software releases.

Tivoli/Sentry v3.0 extends the capabilities of Tivoli/Sentry to the Windows NT platform. The Windows NT operating system is built with counters that can trigger events when a threshold is exceeded. Tivoli/Sentry allows an administrator to select events of interest, set thresholds and then specify automatic corrective actions in response to the predefined conditions. Managers can define availability policies from a central console. Monitors, rules and actions are then automatically deployed to any number of Windows NT servers for an automatic and immediate response to error conditions in accord with established policies. A new monitoring collection is available for Windows 95 and WindowsNT clients.

SECTION 4

RELEASE NOTES

4.1 Tivoli Profiles and DII COE Profiles

Both Tivoli and the DII COE have the concept of "profiles". A Tivoli Profile is not equivalent to a DII COE Profile. The following paragraphs provide a description of each, how they are used in their respective environments, and how they relate.

DII COE Profiles define the user's role (e.g., SSO, watch officer, combat plans office) within their work environment and the system functions associated with that role. DII COE Profiles are assigned to the user by an administrator. The user's default profile is assigned when the user is created in the system; other profiles can be assigned with the DII COE profile management capability. The user may assume one or more profiles during a login session; assumption of a profile allows the user to access, via menus or icons, the system functions associated with the profile in the user's work environment.

A Tivoli Profile is a collection of application-specific information, e.g., user information for Tivoli Admin. Each item in the profile represents a piece of system configuration information, e.g., user's home directory. The information in a profile is specific to the particular profile type, e.g., a User Profile contains user information such as home directory.

Tivoli provides the administrator with a set of default profiles, e.g., Tivoli Admin Default User Profile. Each profile contains a set of default policies and validation policies. Default policies define default values when creating a new profile item, e.g., user's local home directory default is /h/USERS/local/<username>/Scripts. Validation policies define permissible values for profiles items such as the user's password.

A Tivoli Profile Manager is a group of profiles that are subscribed to by a set of system resources, e.g., managed nodes or NIS domains. The system resources are the final destination of the profiles, and hence the profile information. With Tivoli/Admin, the system administrator can distribute user, group and host information to one or more managed nodes and/or NIS/NIS+ domains with the Profile Manager.

The user's COE Profile represents a piece of system configuration information contained in the Tivoli Admin User Profile. Therefore, when an administrator defines a user within a Tivoli User Profile, they also define the user's default COE Profile, just as they would define the user's login name and id.

4.2 Implementation of COE Profiles In Tivoli

In order to accommodate COE Profiles in the Tivoli Management Environment, certain assumptions had to be made during the implementation. These assumptions can be changed by modifying the usage of the COE Profile Database API's in several scripts in the /h/COTS/TIVSRV/Install/UserProfile directory.

DII COE supports the concept of local and global users and profiles. A local user is defined in the /etc style files; whereas a global user is defined in the NIS/NIS+ databases. In the DII COE, a local user may only have local profiles, that is profiles contained within in the system's local profile database. Whereas a global user may only have global profiles, that is profiles contained within the global profile database. The global profile database is then made available (via NFS or some file distribution mechanism such as Tivoli/Courier) to other hosts within the administrative domain. This concept was implemented in the COE to ensure that users have access to profiles and can login even when the Profile Database server is down.

In Tivoli/Admin, since user account information may be distributed to any number of managed nodes and/or NIS/NIS+ domains when the user is created, the concept of local and global becomes blurred. For example, a user account may created locally on five hosts and a NIS domain - is this user then considered to be local or global? In Tivoli, all user's are considered local (for COE Profile purposes) and all user profiles are contained in the local profile database. When a new user is created in the Tivoli User Profile and the User Profile is distributed to one or more managed nodes, the user's COE Profile is also distributed to those nodes.

The Tivoli User and Group Management Guide (Chapter 3) explains how to add new user records. For DII COE V3.0, a new property has been added called the COE Profile. When this property is selected, the corresponding properties panel allows the administrator to select the user's default COE Profile(s). When the user account information is distributed, the user's profile information is also distributed.

4.3 Security Manager Configuration

The /h/AcctGrps/SecAdm/data/config/secman_defaults file is used to set default values and behavior in the DII COE Security Manager. The *modify_accounts* token allows the Security Manager to modify the UNIX user accounts and groups. It should be set to false when other means of manipulating accounts and groups are in use. This token is set to **false** as part of the post-installation for the Tivoli Server and Client segments as DII users and groups will be added via Tivoli/Admin. Further information on these and other tokens in the secman_defaults file can be found in the DII COE Security Manager Administrators Guide, Draft 1, 26 August, 1996.

4.4 User Home Directories and Contents

Tivoli/Admin provides the capability to set the user's home directory and define certain characteristics concerning the user's home directory. Home directories are not created until the administrator distributes the Tivoli User Profile. Tivoli provides a dialog field wherein the

administrator can specify whether the user's home directory is none, local or remotely mounted. The "none" option indicates that there is no home directory. The "local" directory option indicates that the user's home directory will be created on the hosts which have been specified as distribution endpoints. The default user's local home directory is "/h/USERS/local/<username>/Scripts. The "remote" directory option indicates that the user's home directory resides on a mounted file server and is created on the file server when the Tivoli User Profile is distributed. The default user's remote (or global) home directory is "<Server>: /h/USERS/global/<username>/Scripts" where Server is defined as the TME Server. The default value of server may be changed by editing the Server Home Directory Path Default Value in the User Profile Defaults.

4.5 NIS+ Support

Tivoli profiles may be distributed via a Profile Manager to a number of endpoints including another Profile Manager, Tivoli managed nodes, NIS domains and NIS+ domains. Tivoli supports NIS+ as a distribution endpoint and directions for establishing a NIS+ domain endpoint are discussed in Appendix F of the Tivoli User and Group Management Guide.

4.6 User/Group Default and Validation Policies

Appendix E in the Tivoli User and Group Management Guide describes the out-of-the-box default and validation policies provided for user and group management. The following policies have been modified for purposes of DII COE V3.0 in accordance with the DII Security SRS and I&RTS.

UNIX Account Default Policy

Dialog Field	Policy Type	Description
Login Name	Script	Script: COE_default_login name Creates default login name using first character of user's first name and first seven characters of user's last name. If needed the characters are changed to lower case. If the login name generated is not unique, the last character of the login name is dropped and a digit (1-9) is appended.
User Password	Script	Script: COE_default_password Sets the user's default password to a constant value (User2Ch which meets password construction rules in DII Security SRS Note that the user's password must be changed upon initial login.
Pre-Expire Password	Constant	Set to TRUE so that user must change their password upon initial login
Password Aging	Constant	Set to TRUE so that password aging is enabled.
Password	Constant	Sets the maximum password life span to 25 weeks (175 days)

Lifespan		accordance with DII Security SRS.
Global Home Directory	Script	Script: COE_default_hd_server_path Sets the home directory server and path to TME_SERVER:/h/USERS/global/username/Scripts in accordance with DII COE I&RTS. Since the name of the hor directory server is not known apriori, the TME_SERVER is used. This value may be changed by modifying this script.
Local Home Directory	Script	Script: COE_default_hd_local_path Sets the home directory path to h/USERS/local/username/Scripts in accordance with DII COE I&RTS.
Home Directo Contents	Script	Script: COE_default_hd_contents Sets the default location of user configuration files with which to populate a user's home directory to TME_SERVER:/h/data/user_data/Scripts. Since the name of the server is not known apriori, the TME_SERVER is used. This value may be changed by modifying this script.
Not Applicable	Constant	Sets user's home directory permissions to 0750.

UNIX Account Validation Policy

Dialog Field	Policy Type	Description
Login Name	Script	Script: COE_validate_login name Validates that the user's login name is all lower case and no longer than eight characters.
User Password	Script	Script: COE_validate_password Validates that the user's password meets the password construction rules in DII Security SRS.
UID	Script	Script: COE_validate_uid Validates that the user's uid is unique in the TMR and falls between 100 and 60000 (inclusive).
GID	Script	Script: COE_validate_gid Validates that the user's gid is valid and falls between 10 and 60000 (inclusive).

UNIX Group Default Policy

Dialog Field	Policy Type	Description
Group GID	Script	Script: COE_default_group_gid Provides the new account with the next available GID from th ID database between 10 and 60000 (inclusive).

UNIX Group Validation Policy

Dialog Field	Policy Type	Description
Group GID	Script	Script: COE_validate_group_gid Validates that the GID is numeric, greater than or equal to 10 and less than or equal to 60000, and does not start with a "+" sign.

Tivoli allows the administrator to populate the Tivoli User and Group Profiles from the system */etc/passwd* file or NIS databases. If the validation policy for the Tivoli User Profile is enabled during the populate, account information which does not meet the validation policy will be not be imported into the User Profile. For example, if an existing user's password does not meet the password validation policy, the user account will not be imported into the profile. Therefore, when importing user information, you may want to disable validation until the user accounts information can be updated to pass the validation policy.

4.7 Mobile Computing

Tivoli recommends a minimum bandwidth of 19.2kbps (baud) for enterprise-wide environments being managed. However, TME has been implemented in some cases on networks where bandwidth dips to 9600 baud and below. In each of these cases, the performance has been less than optimal due to the available bandwidth.

Tivoli has bandwidth recommendations primarily for performance considerations and not for any physical limits in the product. TME depends on TCP/IP (or Netware/IPX) networks for its communications between systems being managed. The amount of information communicated between systems is significant when such tasks as system monitoring, user management, software distribution are performed across LAN and WAN environments. Tivoli minimizes the overhead incurred over the LAN or WAN by not polling the network in order to gather monitoring information. Tivoli is event driven and reports on an exception basis. The multiplexed distribution service (MDIST) of the Tivoli Management Platform optimizes the use of the network bandwidth as the total available bandwidth has a direct effect on the performance (perceived and real) of any management operation being performed.

4.8 Tivoli and Standards

Tivoli is currently involved in keys standards initiatives and has been delivering products which implement and leverage these specifications in order to maintain flexibility. These standards include SNMP, CORBA, CORBA Common Management Facilities, DMTF/DMI and POSIX.

These standards provide a common way to interchange information, communicate, and interoperate so that the applications solutions need not address these issues directly. These standards are specific to certain areas of technology (e.g., Networking, System Service Calls, Object Request Brokers). Distributed systems management is a very broad discipline and a single standard does not apply since many different service layers are required when implementing these solutions.

Adherence to these standards is a key factor in being able to provide solutions which can span large scale heterogeneous environments. These standards provide the opportunity for many vendors to adhere a single common approach with regard to services when solving these problems and enable to customer to select from multiple solutions providers when implementing a distributed systems management solution.

The initial release of the Tivoli Management Platform was an implementation of the systems management services defined by the OSF/DME. These services were layered on top of an object request broker architecture which enabled the secure, scalable management of distributed compute resources. With the subsequent release of TME 2.0, Tivoli's Management Platform was the first to software product to comply with the CORBA specification. During this same timeframe X/Open and OMG group adopted the Tivoli Management Platform as the basis for their Systems Management standards initiative. Most recently Tivoli has delivered DMTF/DMI compliant solutions for both software distribution and inventory management. The fundamental idea behind DMI is to define a set of well known interfaces with which all

vendors (hardware/software) can interface during software/hardware installation. Tivoli is actively working with leading standards organizations to establish standards for distributed systems management, and is committed to delivering standards based solutions for its customers.

SECTION 5

KNOWN PROBLEMS

No problems other than those described in the product release notes are known at this time.